

Bsafe/Enterprise Security

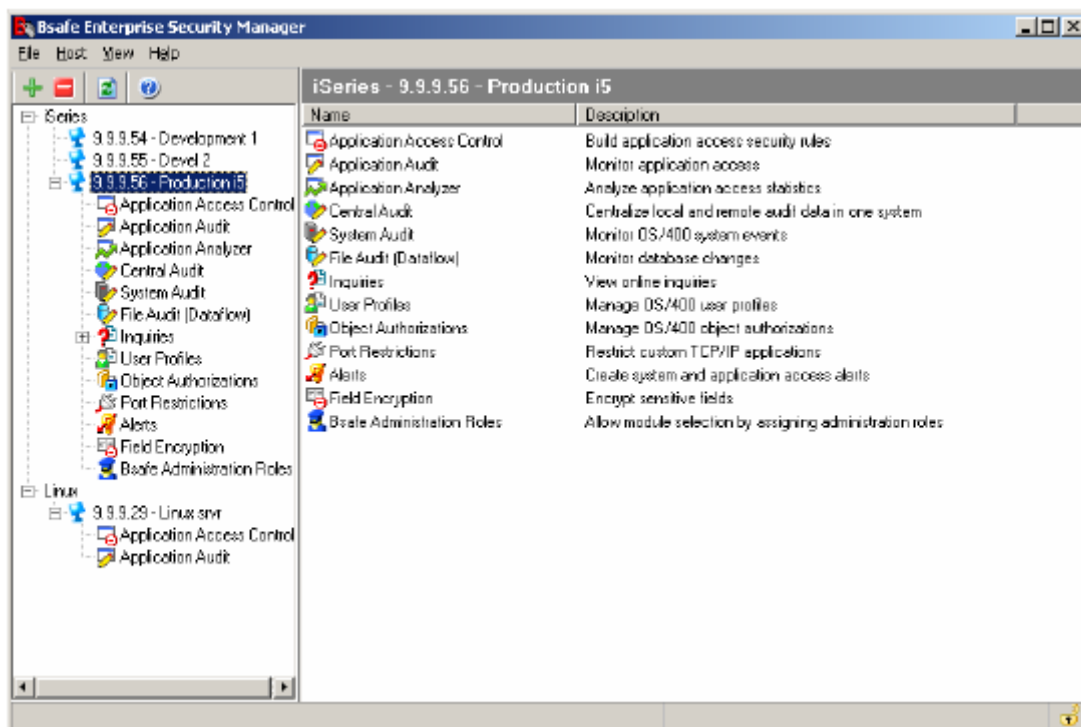
Descripción de la Solución

Contenido

1. Resumen de la Solución
2. Arquitectura
3. Resumen de Cada Módulo
4. Detalle de cada Módulo
5. Beneficios para los Usuarios

1. Resumen de la Solución.

Bsafe/Enterprise Security es una solución completa e integral de seguridad para ambientes multiplataformas – Sistemas i, Linux, Windows y mainframes, que permite prevenir y minimizar el uso indebido de los sistemas. Esto lo realiza en combinación con la protección y control de los puntos salida (“Exit Points”), monitoreo, auditoría, reportes, sistema de alertas IDS y administración general de la seguridad en una consola central a través de una *interfaz gráfica sencilla de administrar*, y bajo la arquitectura Cliente Servidor.

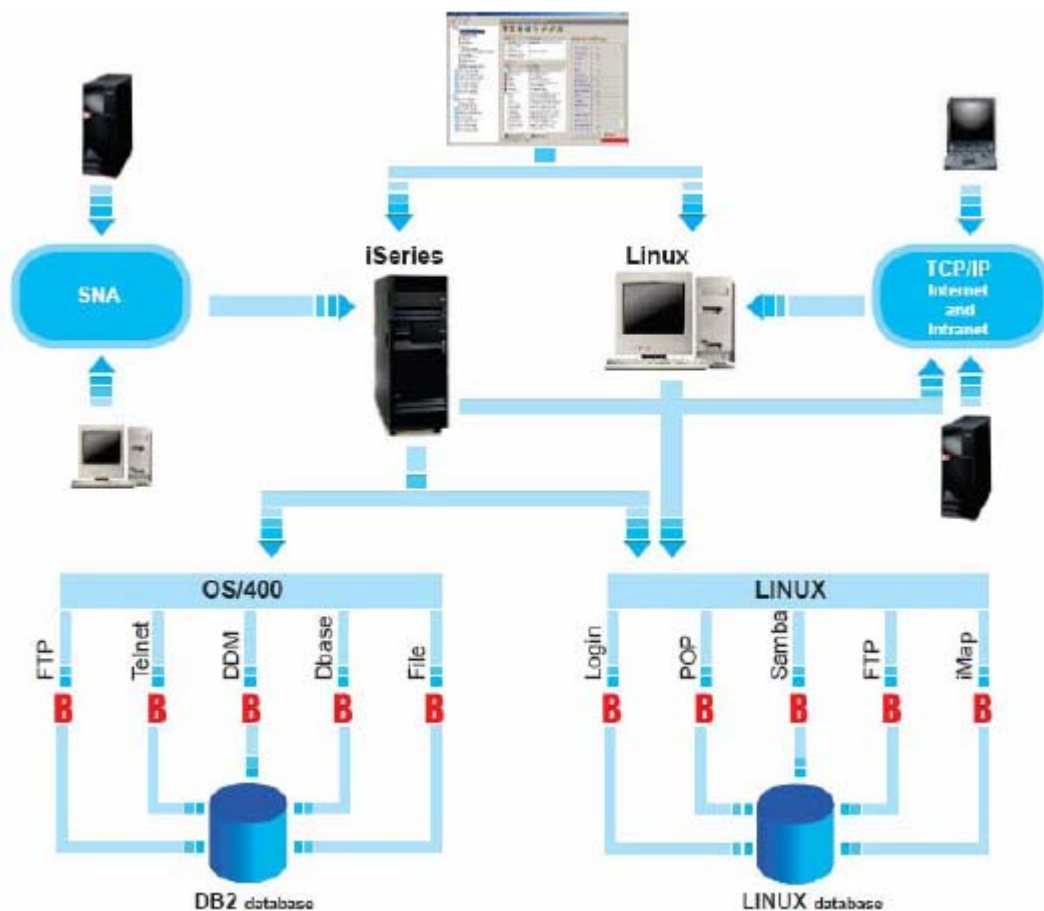


Bsafe/Enterprise Security proporciona las respuestas a los aspectos críticos frente a las propuestas de nuestros ejecutivos en las organizaciones y a los requerimientos del personal de seguridad que día a día tienen que cumplir con una serie de regulaciones de conformidad con la ley.

2. Arquitectura.

Bsafe/Enterprise Security está basada en una Arquitectura cliente/servidor. El software encargado de la protección principal y el manejador de reportes reside internamente en el sistema i proporcionando una protección nativa, mientras que las definiciones y el control es manejado a través de una interfaz GUI, amigable e intuitiva desde uno o más PC's desde la red.

No se utilizan conexiones ODBC en las conexiones cliente/servidor, por lo que las funciones ODBC pueden ser restringidas sin afectar la operación de la consola GUI. La conexión a través de la consola puede utilizar el protocolo de seguridad SSL para las conexiones cliente/servidor.



3. Resumen de Cada Módulo o Funcionalidad.



Interfaz GUI de la Consola de Administración Basada en Windows. La Seguridad es controlada de una manera sencilla, con ayuda en línea.



Control de Acceso a las Aplicaciones para los Sistemas I y Linux incluyendo:

- Permisos por grupos
- Control por usuarios y direcciones IP
- Intercambio autorizaciones de usuarios "Account swapping"
- Control de tiempo para autorizaciones
- Replicación de configuración a través de múltiples servidores
- Protección de archivos contra usuarios poderosos (QSECOFR, usuarios con autorización especial *ALLOBJ)
- Sub módulo opcional para Linux



Auditoria de las Aplicaciones. Funcionalidad para el registro y visualización de las anotaciones de trabajo y auditoria de todos los eventos de accesos.



Analizador del Tráfico de la Red. Interfaz gráfica que permite analizar el tráfico de la red.



Auditoria de Archivos. Monitor de auditoria de archivos a nivel de archivos y campos. Es un monitor de Integridad de datos que muestra los cambios en la base de datos a nivel de campos.



Auditoria del Sistema. Control de las políticas de diario del sistema, visualización de los eventos y reportes.



Consultas y Generación de Reportes poderoso. Consultas y Reportes en línea sobre configuraciones del sistema, autorizaciones, accesos, y eventos.



Administrador de Perfiles de usuario. Administrador eficaz y efectivo de los perfiles de usuarios del sistema i.



Administrador de los Objetos del Sistema i. Administrador de las autorizaciones de los objetos del sistema i.



Administrador para la Restricción de Puertos del Sistema i. Manejo de la restricción de puertos del sistema i.



Alertas. Sistema de Detección de Intrusos (IDS) para los eventos de la red y del sistema.



Encriptación de Campos y Protección de Archivos. Mantener encriptados los campos críticos de los archivos claves de la organización, y proteger los archivos contra los usuarios poderosos (QSECOFR o un usuario con Autorización *ALLOBJ).



Administración de los Roles de la Organización. Otorgar las funciones a los administradores de la solución de forma granular.



Auditoría Centralizada. Consolidación de la auditoría permitiendo obtener información desde muchas fuentes de auditoría incluyendo registros leídos de un archivo.

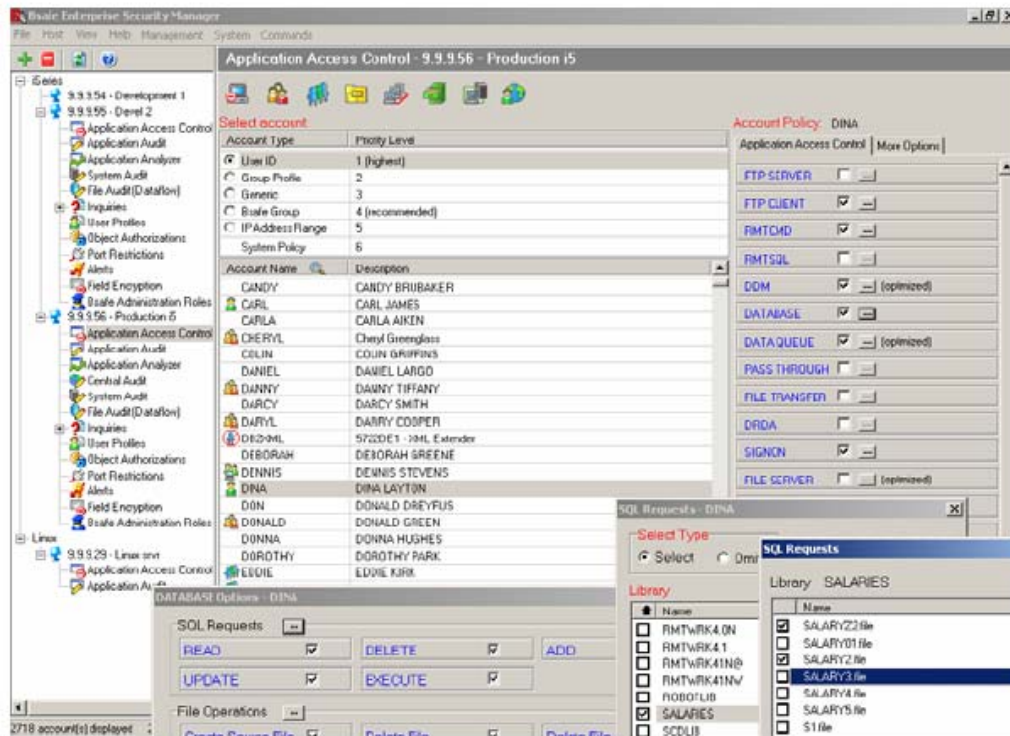


Manejo de Inactividad de Sesiones y de Usuarios. Control de tiempo de inactividad de sesiones y usuarios, configurado por usuarios, grupos y permitiendo definir diferentes tipos de acciones.

Análisis de Vulnerabilidad. Permite la generación de un informe con todos los riesgos actuales y algunas sugerencias para resolver estos riesgos.

4. Detalle de cada Módulo

4.1. Consola de Administración basada en Windows (GUI).



Bsafe/Enterprise Security es controlada a través de una consola centralizada basada en un cliente Windows con una interfase GUI conectada al sistema i. Ofrece una interfaz gráfica amigable al usuario, operaciones que se realizan con un solo click y ayuda en línea. A través de una simple pantalla, se pueden manejar todos los sistemas i y LPAR's configurados en nuestra red de forma simultánea.

Suporte SSL y Acceso Criptográfico

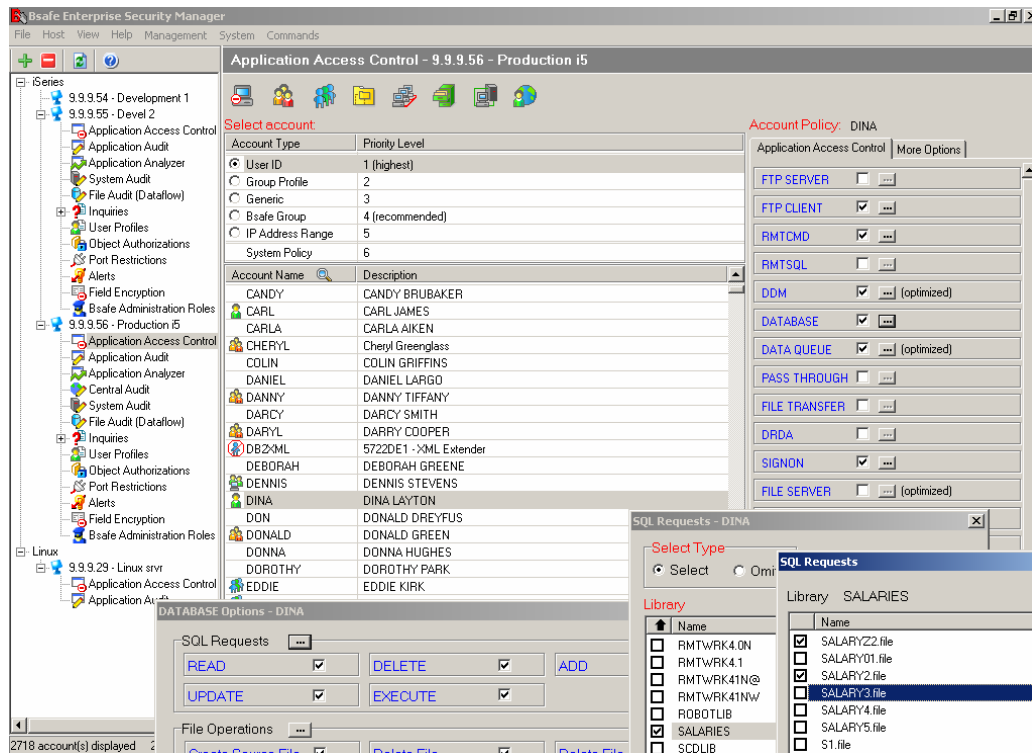
Bsafe/Enterprise Security incluye soporte SSL e intercambio de datos de forma encriptada entre los PC clientes y el OS/400, a través de TCP/IP. Esto es realizado a través de la integración de los Programas bajo Licencia de IBM Digital Certificate Manager e IBM Crypto Access Provider para OS/400.

Suporte de Cualquier Lenguaje Nacional

Las bases de **Bsafe/Enterprise Security** soportan cualquier lenguaje nacional soportado por los archivos del sistema OS400 incluyendo DBCS (double-byte character set). Adicionalmente, la interfase GUI puede ser configurada para cualquier lenguaje soportado por el PC.

4.2. Control de Acceso a las Aplicaciones.

Control de acceso a los servidores de aplicaciones del sistema i a través de los puntos de salida “Exit Points”.



El acceso a las aplicaciones TCP/IP es controlado a través del Sistema de Prevención de Intrusos (IPS) de **Bsafe/Enterprise Security** utilizando los puntos de salidas “Exit Points” y otras tecnologías. Esta funcionalidad provee un control flexible pero firme para prevenir los requerimientos de acceso no autorizados a través de conexiones TCP/IP y SNA. El acceso puede ser restringido por usuario, grupo, dirección IP, aplicación servidor/servicio y operaciones específicas. La variedad de servidores de aplicaciones y servicios del sistema i protegidos por **Bsafe/Enterprise Security** incluyen:

Sobre TCP/IP:

Telnet, FTP, TFTP, Comandos Remotos, SQL Remotos, Base de Datos, Colas de Datos, Acceso ODBC, DDM, DRDA, IFS, Signon, Servidor de Archivos, Servidor Central, Servidor de Mensajes, Impresión Virtual, Impresión de Red, Inicio de Sesión sobre WSG y más.

Sobre SNA:

DDM, Paso a través, Cola de Datos, Transferencia de Archivos y DRDA.

Sobre el Sistema: (IMPORTANTE)

Eliminación de receptores de diario, Apagado del Sistema "Power Down System", Tecla de Atención del Sistema, Cambio de Atributos de Archivos de Impresión, Finalización de Trabajos, Control de TCP/IP, Arrancar SQL, Arrancar DFU, Ejecutar actualización de datos, Arranque y finalización de Subsistemas, Otorgar y revocar autorizaciones, Cambiar la configuración de una línea de comunicaciones, controlar la doble sesión, Controlar las instrucciones internas del SQL.

El acceso puede ser asegurado bajando a nivel de de una acción simple por ejemplo eliminación en un FTP, una sentencia "select" en una ejecución SQL y comandos del OS400. A nivel de objetos, el acceso puede ser controlado para dispositivos específicos, bibliotecas, archivos, comandos, programas y vías de acceso del IFS.

Control de Acceso de Usuarios de Internet

Bsafe/Enterprise Security permite administrar los usuarios públicos de Internet para las aplicaciones del sistema i basadas en web. Esta funcionalidad incluye la creación, actualización y eliminación de las listas de validación de objetos y asignación de y eliminación de usuarios y contraseñas.

Protección sobre Archivos

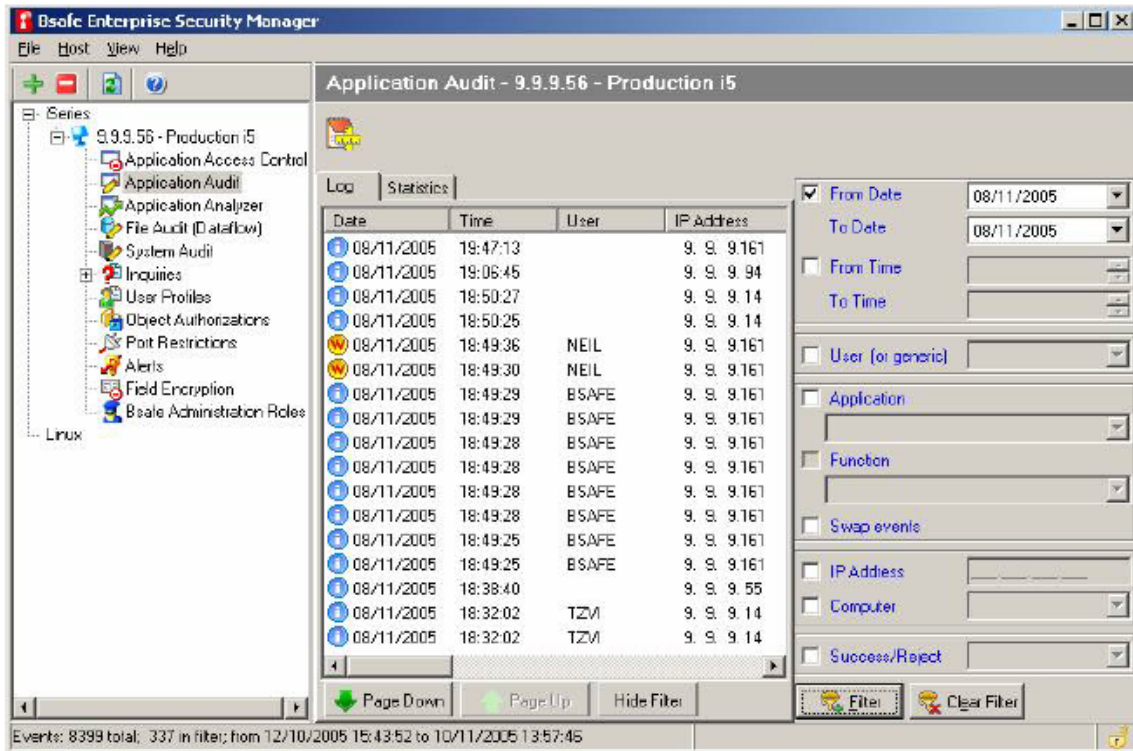
La funcionalidad de control de acceso sobre los archivos del sistema i permite otorgar una autorización por encima de la seguridad del sistema operativo del OS/400, permitiendo restringir inclusive archivos críticos de los usuarios poderosos que tengan la autorización especial *ALLOBJ o inclusive el usuario QSECOFR.

Intercambio de Autorizaciones de Usuarios

La funcionalidad de intercambio de autorizaciones de usuarios de **Bsafe/Enterprise Security** permite otorgar autorizaciones de usuarios de forma temporalmente a otros usuarios o grupos de usuarios sobre objetos del OS/400 o permisos sobre la red. El usuario o grupo de usuarios recibe la autorización del otro usuario sin requerir conocer su contraseña manteniendo la seguridad.

4.3. Auditoria de Aplicaciones.

Anotaciones detalladas y Auditoria de los Eventos de Accesos

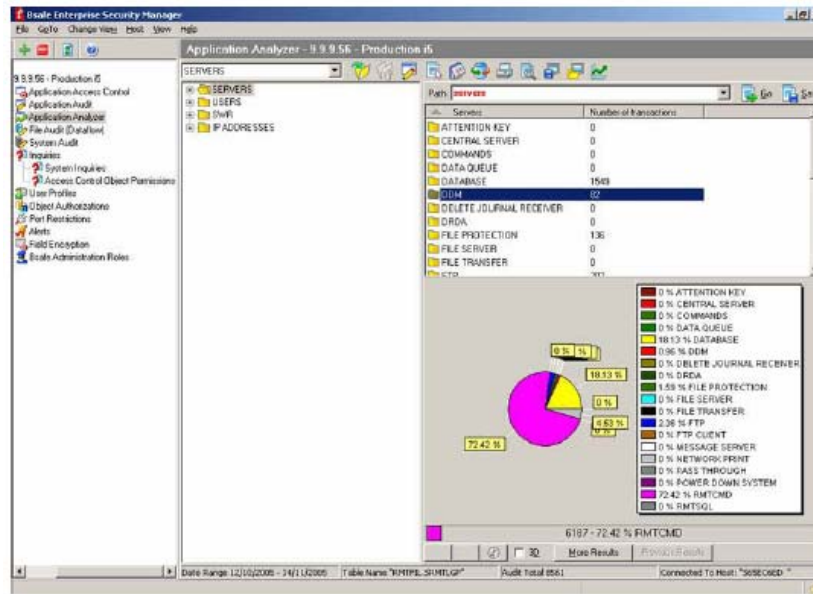


The screenshot displays the Bsafe Enterprise Security Manager interface. The main window is titled "Application Audit - 9.9.9.56 - Production i5". On the left, a tree view shows the hierarchy of security features, with "Application Audit" selected. The central pane shows a log table with columns for Date, Time, User, and IP Address. The right pane contains various filter options such as From Date, To Date, User, Application, Function, and Success/Reject.

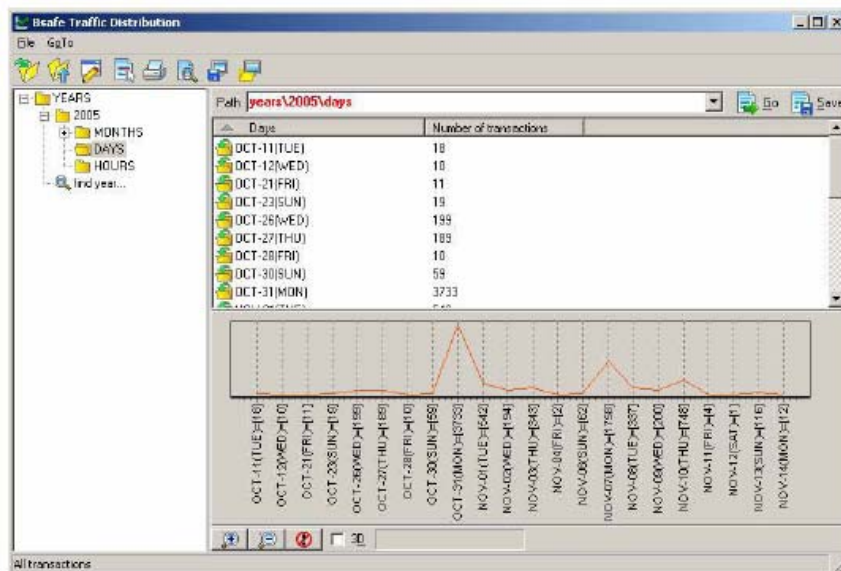
Date	Time	User	IP Address
08/11/2005	19:47:13		9. 9. 9.161
08/11/2005	19:06:45		9. 9. 9. 94
08/11/2005	18:50:27		9. 9. 9. 14
08/11/2005	18:50:25		9. 9. 9. 14
08/11/2005	18:49:36	NEIL	9. 9. 9.161
08/11/2005	18:49:30	NEIL	9. 9. 9.161
08/11/2005	18:49:29	BSAFE	9. 9. 9.161
08/11/2005	18:49:29	BSAFE	9. 9. 9.161
08/11/2005	18:49:28	BSAFE	9. 9. 9.161
08/11/2005	18:49:28	BSAFE	9. 9. 9.161
08/11/2005	18:49:28	BSAFE	9. 9. 9.161
08/11/2005	18:49:28	BSAFE	9. 9. 9.161
08/11/2005	18:49:28	BSAFE	9. 9. 9.161
08/11/2005	18:49:25	BSAFE	9. 9. 9.161
08/11/2005	18:49:25	BSAFE	9. 9. 9.161
08/11/2005	18:38:40		9. 9. 9. 55
08/11/2005	18:32:02	TZM	9. 9. 9. 14
08/11/2005	18:32:02	TZM	9. 9. 9. 14

En esta funcionalidad se registra toda la actividad de la red, de los puntos de salida e información vital que no es registrada por el sistema operativo de forma nativa. Este registro incluye detalles tales como: dirección IP, usuario, archivo, biblioteca, transacción FTP, sentencia SQL. La información es registrada inmediatamente que se produce el evento, es decir, la auditoria es en línea. Se ofrecen diferentes criterios para filtrar la información y se ofrece una gran variedad de reportes.

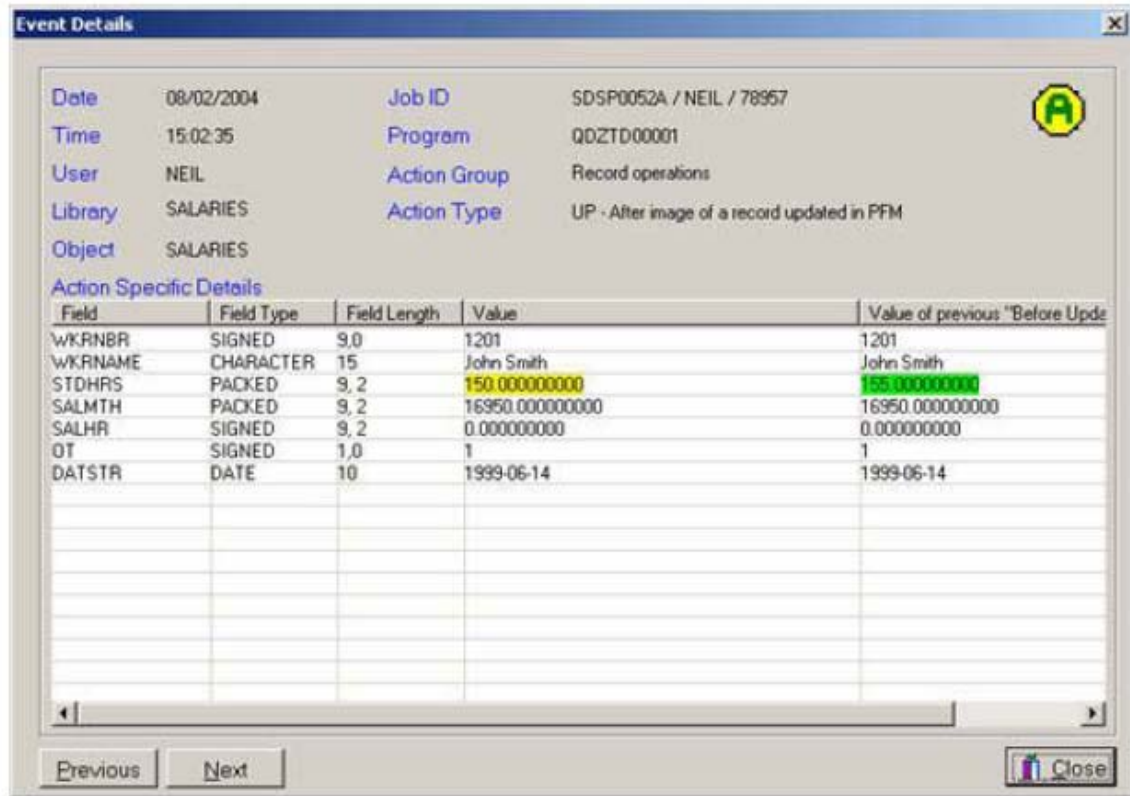
4.4 Analizador Gráfico para el Tráfico de las Aplicaciones Red.



Todos los eventos de la red y de los puntos de salida registrados en la funcionalidad de la Auditoria de Aplicaciones, están también disponibles para esta funcionalidad llamada Análisis Gráfico del tráfico de la Red, la cual permite un análisis a través de un sistema sofisticado de forma gráfica y a través de diferentes criterios de filtros. Los gráficos y tablas del Analizador de **Bsafe/Enterprise Security**, pueden ser revisados y obtener información específica sobre eventos específicos. Esto proporciona una gráfica real sobre la tendencia de la red, ayudando a identificar cualquier actividad anormal, para tomar cualquier decisión en temas de seguridad, costos entre otros.



4.5. Auditoria sobre Archivos. (Monitor de Integridad de datos)



The screenshot shows a window titled "Event Details" with the following information:

- Date: 08/02/2004
- Time: 15:02:35
- User: NEIL
- Library: SALARIES
- Object: SALARIES
- Job ID: SDSP0052A / NEIL / 78957
- Program: QDZTD00001
- Action Group: Record operations
- Action Type: UP - After image of a record updated in PFM

Below this information is a table titled "Action Specific Details" with the following data:

Field	Field Type	Field Length	Value	Value of previous "Before Update"
WKRNR	SIGNED	9,0	1201	1201
WKRNAME	CHARACTER	15	John Smith	John Smith
STDHRS	PACKED	9,2	150.00000000	150.00000000
SALMTH	PACKED	9,2	16950.00000000	16950.00000000
SALHR	SIGNED	9,2	0.00000000	0.00000000
OT	SIGNED	1,0	1	1
DATSTR	DATE	10	1999-06-14	1999-06-14

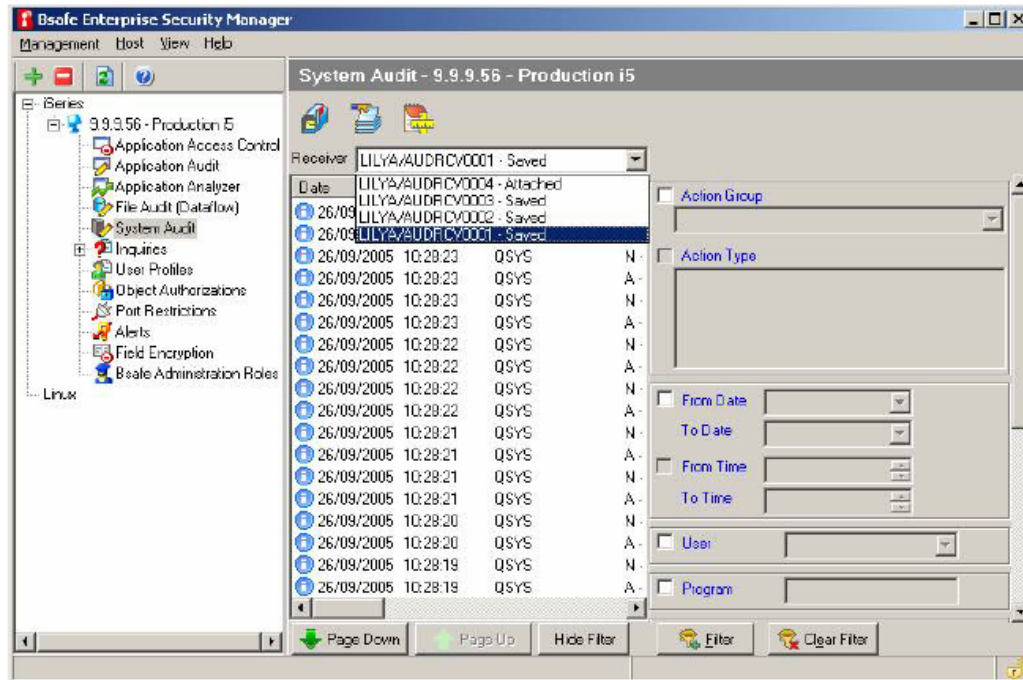
The window also includes "Previous" and "Next" buttons at the bottom left and a "Close" button at the bottom right.

Con el monitor de integridad de auditoria y seguridad de archivos de **Bsafe/Enterprise Security**, (Dataflow) se pueden registrar todos los cambios de los datos críticos de la organización a nivel de campos. Los valores de los campos pueden ser visualizados acompañados del anterior y posterior y una descripción completa del ambiente en el que se ejecutó el cambio incluyendo el usuario, el programa a través que se realizó y más.

Esta funcionalidad fue diseñada para usuarios que no tengan conocimientos profundos de los comandos del sistema. Fácilmente se puede identificar el valor de los campos y los valores cambiados.

La funcionalidad de Auditoria de Archivos de **Bsafe/Enterprise Security** puede identificar rápidamente los cambios realizados asistirlo en la toma de decisiones ante brechas de seguridad y en la restauración de datos corruptos.

4.6. Auditoria del Sistema.



La funcionalidad de Auditoria del Sistema de **Bsafe/Enterprise Security** es una herramienta innovadora con interfaz gráfica GUI la cual permite visualizar las entradas de auditoria del sistema.

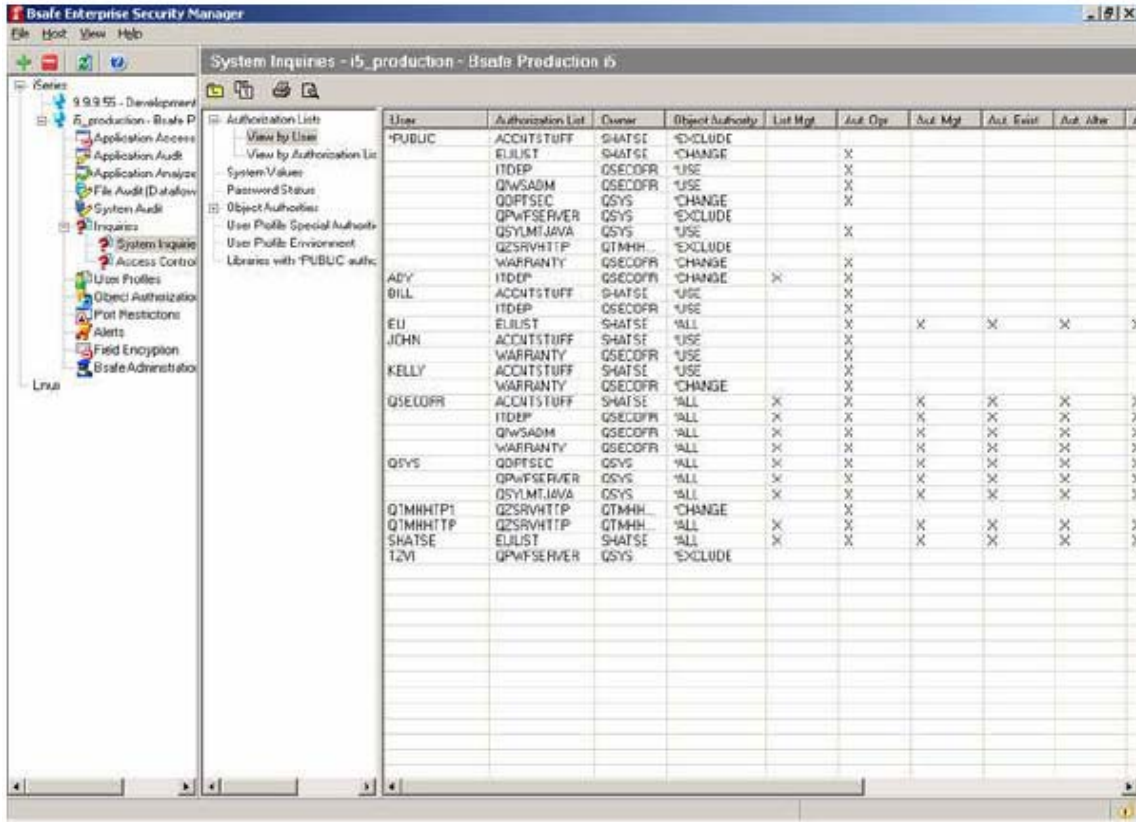
Esta proporciona una supervisión completa del diario del sistema incluyendo administración de los receptores de diario, definición de las políticas de auditoria, visualización en línea y emisión de reportes, abarca docenas de reportes predefinidos y adicionalmente proporciona un generador de reportes para crear reportes personalizados.

El visualizador interactivo de diario del sistema proporciona filtros a través de diferentes criterios. Facilita la investigación e brechas de seguridad evita realizar las tareas complicadas de revisar los receptores de diarios del sistema de forma nativa.

El generador de reportes permite crear reportes personalizados basados en diferentes criterios de selección. Los reportes pueden ser ejecutados en línea o planificados.

Las Políticas de Auditoria del Sistema pueden ser cambiadas con un solo click, a nivel usuario, de objetos y a nivel del sistema.

4.7 Consultas y Generación de Reportes poderoso



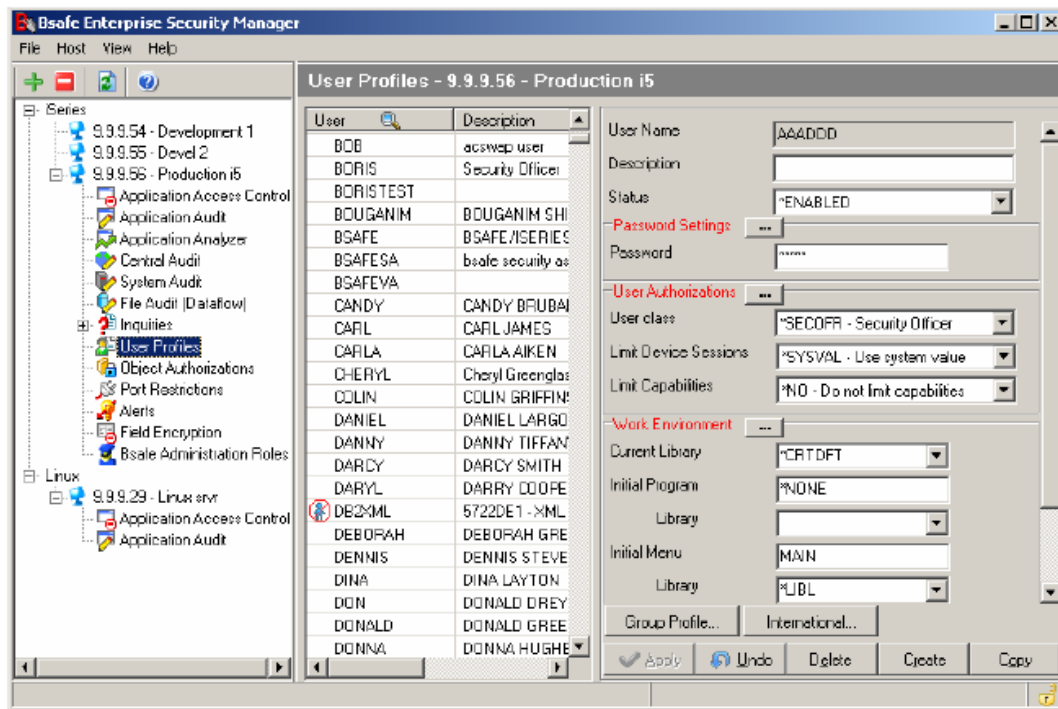
User	Authorization List	Owner	Object Authority	List Mgt	Aut. Ope	Aut. Mgt	Aut. Excl	Aut. Alter	
*PUBLIC	ACCNSTUFF	SHATSE	*EXCLUDE						
	ELJLIST	SHATSE	*CHANGE		X				
	ITDEP	QSECOFR	*USE			X			
	QWNSADM	QSECOFR	*USE			X			
	QDFSEC	QSYS	*CHANGE			X			
	QPWFSEVR	QSYS	*EXCLUDE						
	QSYLMTJAVA	QSYS	*USE		X				
	Q2SRVHTP	QTMHH	*EXCLUDE						
	WARRANTY	QSECOFR	*CHANGE		X				
ADY	ITDEP	QSECOFR	*CHANGE	X					
BILL	ACCNSTUFF	SHATSE	*USE			X			
	ITDEP	QSECOFR	*USE			X			
EJ	ELJLIST	SHATSE	*ALL			X	X	X	X
JOHN	ACCNSTUFF	SHATSE	*USE			X			
	WARRANTY	QSECOFR	*USE			X			
KELLY	ACCNSTUFF	SHATSE	*USE			X			
	WARRANTY	QSECOFR	*CHANGE			X			
QSECOFR	ACCNSTUFF	SHATSE	*ALL	X	X	X	X	X	X
	ITDEP	QSECOFR	*ALL	X	X	X	X	X	X
	QWNSADM	QSECOFR	*ALL	X	X	X	X	X	X
	WARRANTY	QSECOFR	*ALL	X	X	X	X	X	X
QSYS	QDFSEC	QSYS	*ALL	X	X	X	X	X	X
	QPWFSEVR	QSYS	*ALL	X	X	X	X	X	X
	QSYLMTJAVA	QSYS	*ALL	X	X	X	X	X	X
QTMHHTP1	Q2SRVHTP	QTMHH	*CHANGE		X				
QTMHHTP	Q2SRVHTP	QTMHH	*ALL	X	X	X	X	X	X
SHATSE	ELJLIST	SHATSE	*ALL	X	X	X	X	X	X
TZVI	QPWFSEVR	QSYS	*EXCLUDE						

Esta funcionalidad ofrece reportes en línea sobre autorizaciones de objetos y usuarios para ayudar a identificar y cerrar cualquier riesgo de seguridad en la definición de la configuración del sistema.

Todas las consultas se ejecutan desde la interfaz gráfica GUI en tiempo real en el servidor. Esto proporciona a los administradores un conjunto de herramientas valiosas que permiten identificar cualquier vulnerabilidad en el sistema i.

La suite de consultas proporciona una variedad de reportes al instante tales como: listas de autorización por objeto y por usuario, valores del sistema, su descripción y valores recomendados. Otras consultas están relacionadas con usuarios, ambiente de trabajo, configuración de políticas, contraseñas, autorizaciones especiales y autorizaciones sobre bibliotecas.

4.8. Administración de Perfiles de Usuario.

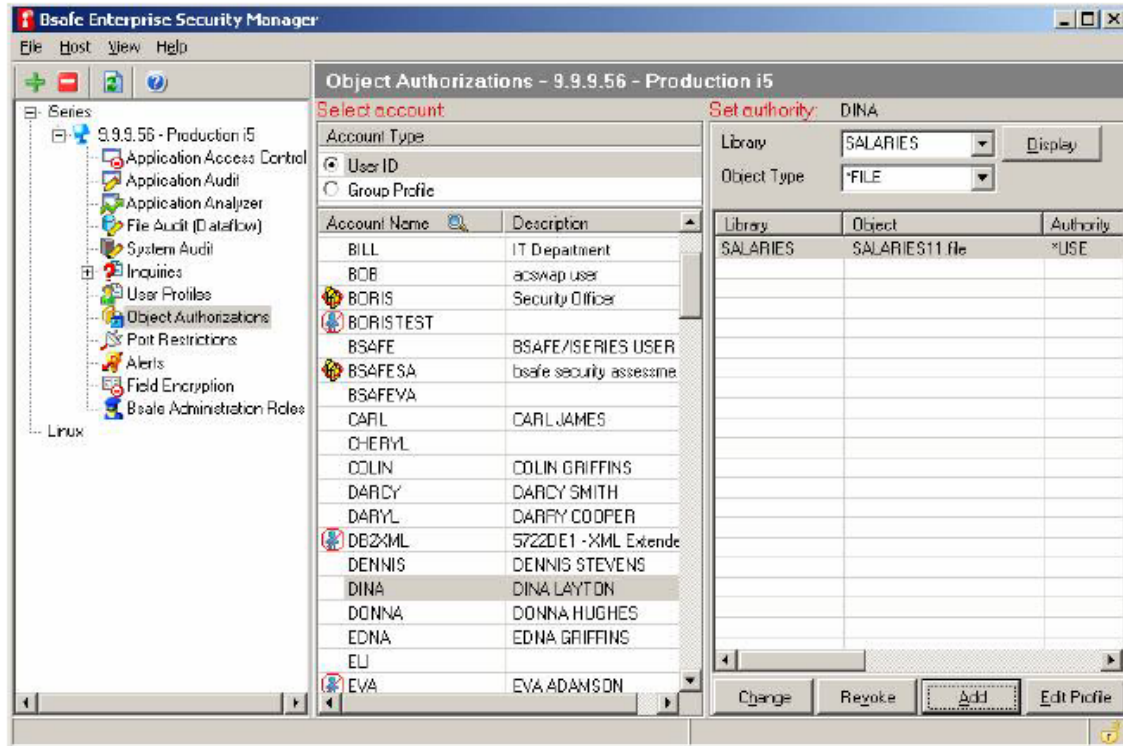


Esta funcionalidad permite la administración gráfica y poderosa de los perfiles de usuario del sistema operativo OS/400. Proporciona a los administradores una manera fácil e intuitiva de crear, mantener y administrar los perfiles de usuario del sistema i.

Se muestra la lista de usuarios completa en un lado de la pantalla incluyendo el perfil de usuario, el estado y su descripción, y del otro lado se muestra toda la información del usuario seleccionado.

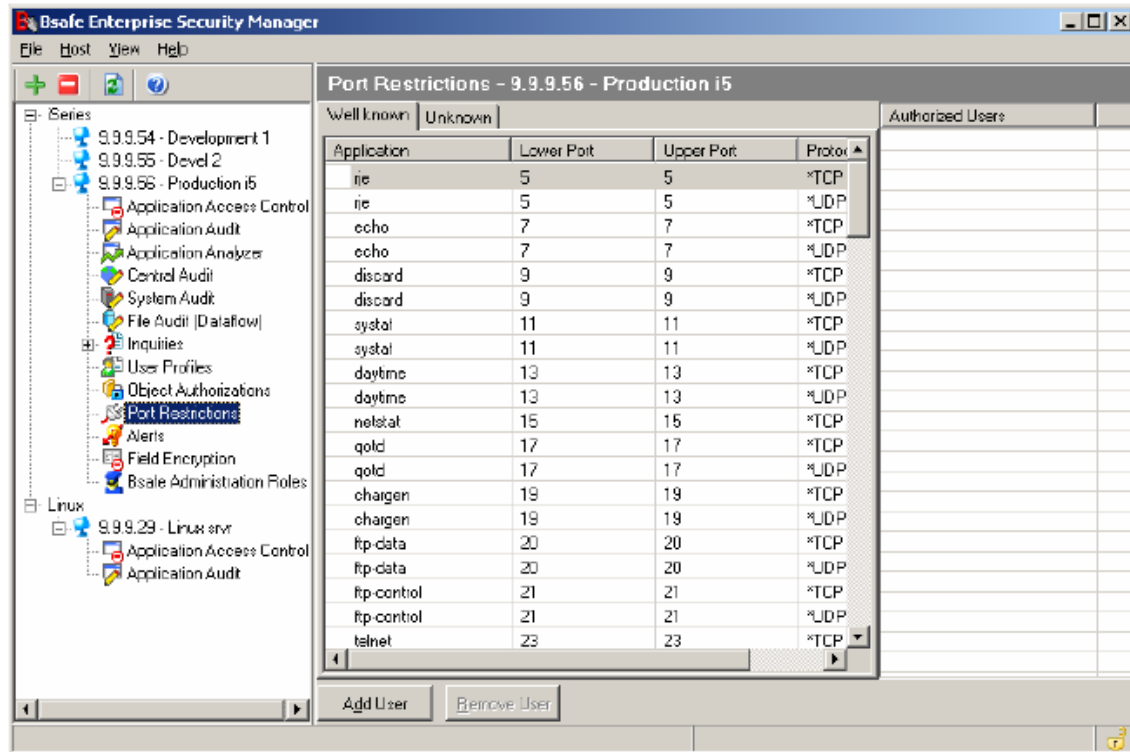
El énfasis en esta funcionalidad, es el uso y la eficiencia para el administrador por ejemplo se muestran la lista de los perfiles de grupos cuando se va a asignar un grupo a un perfil de usuario.

4.9. Autorizaciones de Objetos.



Con **Bsafe/Enterprise Security** se tienen una solución flexible, fácil de utilizar y eficiente para administrar los permisos de usuarios y autorizaciones sobre los objetos del sistema i.

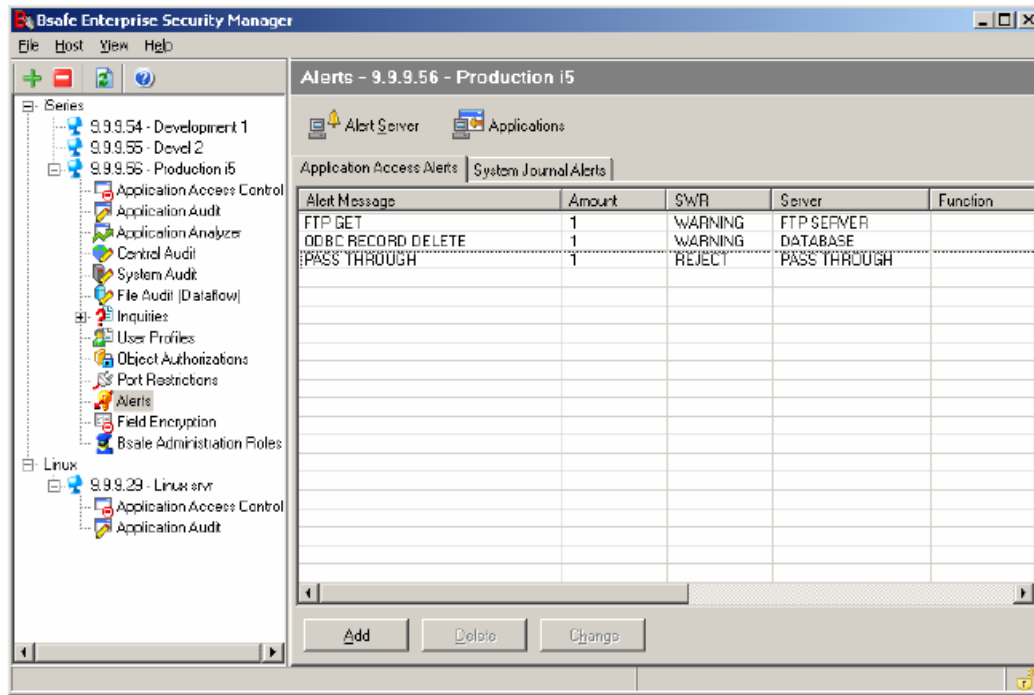
4.10. Administración de la Restricción de Puertos.



Esta funcionalidad permite restringir el acceso a los puertos del sistema i por aplicación, por protocolo, por usuarios autorizados de una forma simple a través de una interfaz gráfica GUI.

La solución lista todos los puertos conocidos en detalle para reducir el riesgo de errores no intencionales en las definiciones. Los rangos de puertos no conocidos pueden ser restringidos para usuarios específicos de una forma sencilla.

4.11. Alertas, Sistema de Detección de Intrusos (IDS).



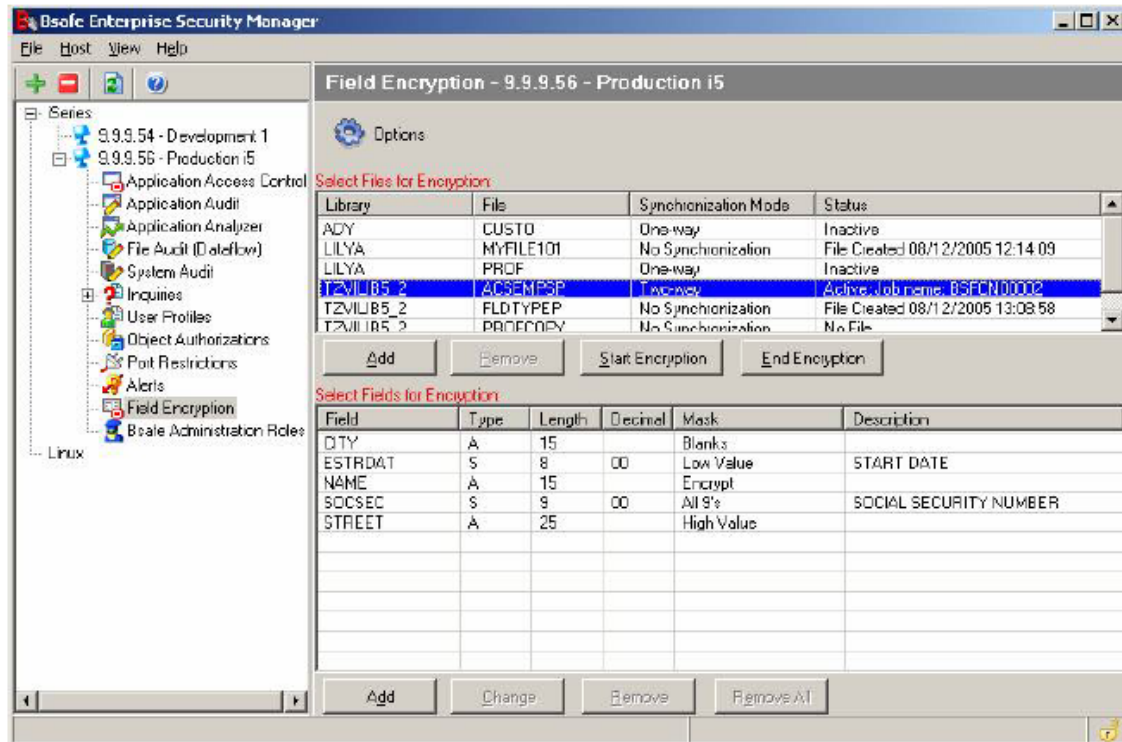
Esta funcionalidad permite que las alertas se envíen en tiempo siguiendo la actividad de los eventos no autorizados sobre la o eventos del sistema. En el momento en que ocurre un evento en el sistema se envía una notificación en tiempo real vía un mensaje pop-up al PC, e-mail, SMS, SNMP o a una aplicación externa.

Bsafe/Enterprise Security actualmente soporta enviar mensajes sobre SNMP para los siguientes productos: IBM-Tivoli, HP-Openview, CA-Unicenter, Orange-Cellular, IBMTeledrine.

La flexibilidad del IDS permite alertar diferentes tipos de eventos tales como: accesos DRDA y eventos específicos como lecturas ODBC.

Bsafe/Enterprise Security permite adicionalmente definir alertas del sistema. Se pueden obtener mensajes de forma instantánea de todos los tipos de eventos del sistema tales como intentos no válidos de sesión para un sistema o para un usuario específico, cambios en los valores del sistema y más.

4.12. Encriptación a Nivel de Campos y Protección de Archivos.



Encriptación de Campos:

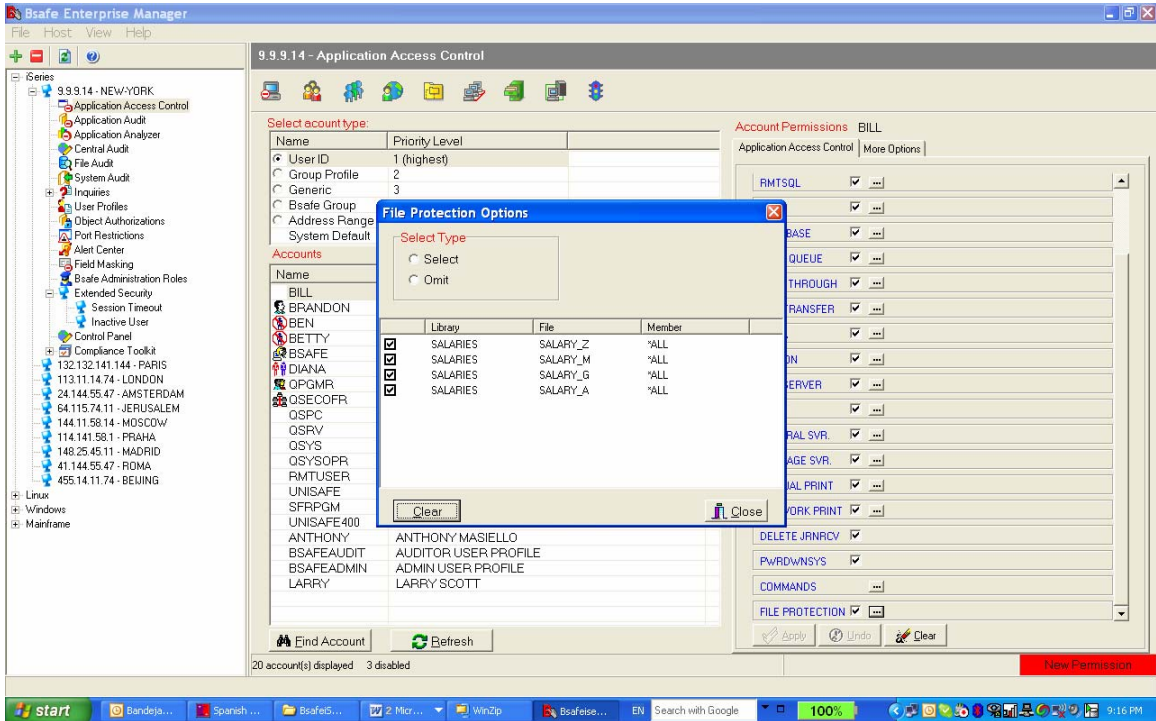
Bsafe/Enterprise Security permite implementar enmascarar campos de las bases de datos del sistema i, a través de la encriptación y colocación de máscaras en los campos. A través de esta tecnología, se proporciona acceso a ciertos campos y a otros no.

Una vez implementado, el campo encriptado no puede ser visualizado por los usuarios ni modificado por ninguna aplicación.

La solución permite controlar cuando los campos pueden ser actualizados o no por las aplicaciones.

Protección de Archivos:

Bsafe/Enterprise Security permite proteger los archivos contra usuarios poderosos como por ejemplo QSECOFR, o contra usuarios con autorizaciones especiales *ALLOBJ

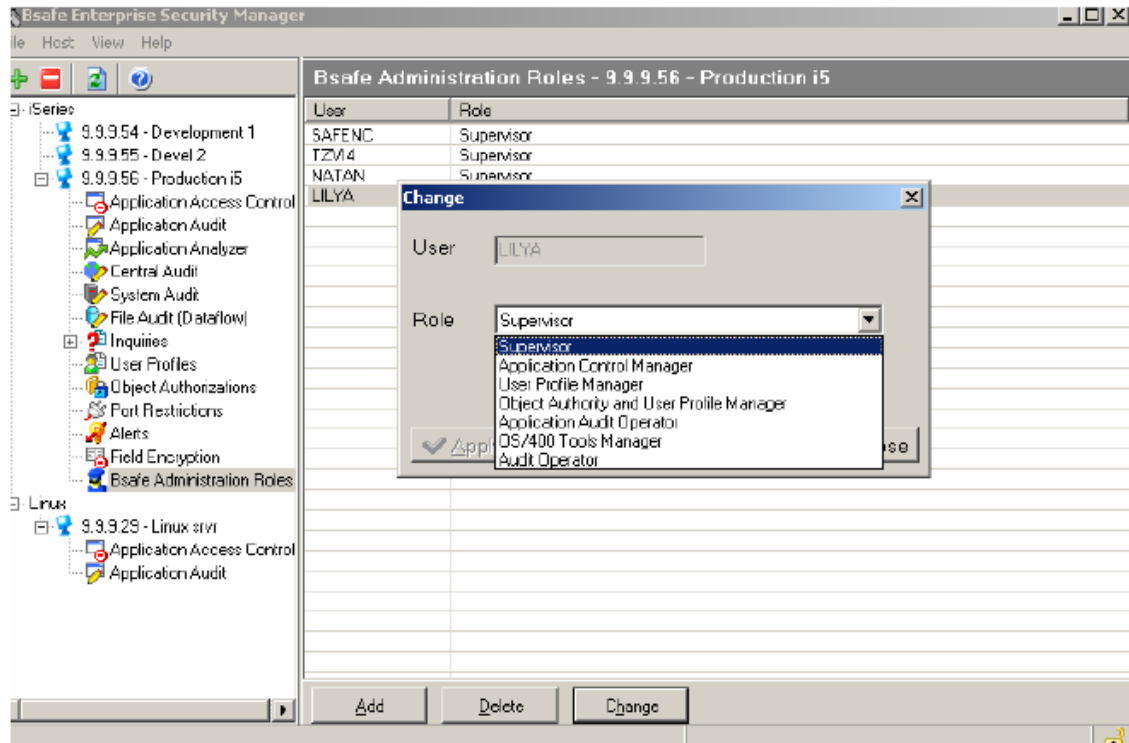


The screenshot shows the Bsafe Enterprise Manager interface. A dialog box titled "File Protection Options" is open, displaying a table of accounts and their associated file protection settings. The dialog has two radio buttons: "Select" (which is selected) and "Omit".

Account Name	Library	File	Member	
BEN	<input checked="" type="checkbox"/>	SALARIES	SALARY_Z	*ALL
BETTY	<input checked="" type="checkbox"/>	SALARIES	SALARY_M	*ALL
DIANA	<input checked="" type="checkbox"/>	SALARIES	SALARY_G	*ALL
QPGMR	<input checked="" type="checkbox"/>	SALARIES	SALARY_A	*ALL
QSECOFR	<input checked="" type="checkbox"/>	SALARIES	SALARY_A	*ALL
OSPC	<input type="checkbox"/>			
OSRV	<input type="checkbox"/>			
OSYS	<input type="checkbox"/>			
OSYSOPR	<input type="checkbox"/>			
RMTUSER	<input type="checkbox"/>			
UNISAFE	<input type="checkbox"/>			
SFRPFGM	<input type="checkbox"/>			
UNISAFE400	<input type="checkbox"/>			
ANTHONY	<input type="checkbox"/>	ANTHONY MASIELLO		
BSAFEAUDIT	<input type="checkbox"/>	AUDITOR USER PROFILE		
BSAFEADMIN	<input type="checkbox"/>	ADMIN USER PROFILE		
LARRY	<input type="checkbox"/>	LARRY SCOTT		

The background window shows the "Accounts" list with various user profiles and their details. The "File Protection Options" dialog is currently focused on the "Select" option, indicating that file protection is being applied to the selected accounts.

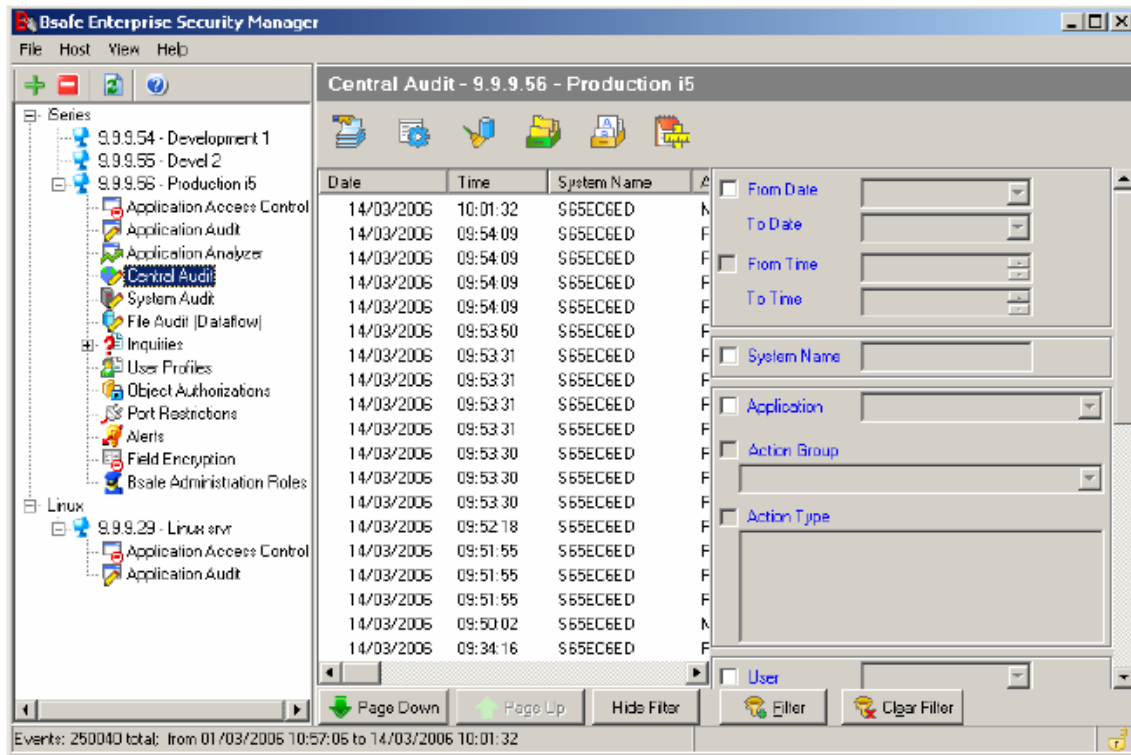
4.13. Manejo de los Roles de Administradores



A través de la funcionalidad de Manejo de los Roles de Administración de **Bsafe/Enterprise Security** se pueden distribuir las diferentes tareas de seguridad en los distintos miembros del equipo de administradores.

Cuando se diseña el role seleccionado, ese role debe tener funciones específicas. Esta poderosa característica permite mantener una clara separación entre la administración de los perfiles de usuario, las políticas de auditoría del sistema, los permisos de red, y el control de las autorizaciones sobre los objetos y dividirlos según las necesidades de la organización.

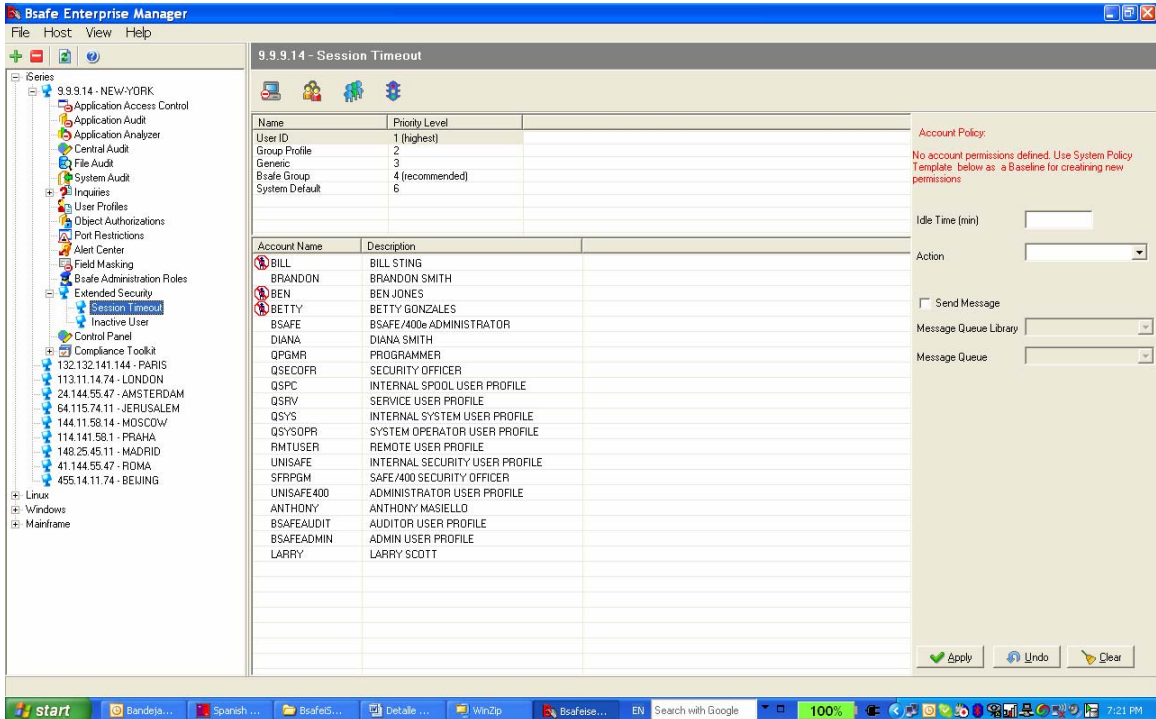
4.14. Auditoria Centralizada y Consolidación de Anotaciones.



La auditoria centralizada proporciona información centralizada y consolidada desde varias fuentes de información. La información de los diarios del sistema y de archivos se puede extraer cuando se eliminan los receptores y colocarla en este repositorio centralizado. Otra fuente de información es la extraída a través del acceso a la red.

La combinación de múltiples fuentes de información y la posibilidad de filtrar la información a través de múltiples criterios tales como aplicación, usuario, y tiempo hacen de la funcionalidad de Auditoria Centralizada y Consolidación de Anotaciones, una herramienta de auditoría realmente poderosa.

4.15. Manejo de Inactividad de Sesiones y Usuarios.



The screenshot shows the Bsafe Enterprise Manager interface. The left sidebar displays a tree view of the system configuration, with 'Session Timeout' selected under the 'User Profiles' section. The main window displays the configuration for '9.9.9.14 - Session Timeout'. It includes a table for 'Priority Level' and a table for 'Account Name' and 'Description'.

Name	Priority Level
User ID	1 (highest)
Group Profile	2
Generic	3
Bsafe Group	4 (recommended)
System Default	6

Account Name	Description
BILL	BILL STING
BRANDON	BRANDON SMITH
BEN	BEN JONES
BETTY	BETTY GONZALES
BSAFE	BSAFE/400e ADMINISTRATOR
DIANA	DIANA SMITH
QPGMR	PROGRAMMER
QSECDFR	SECURITY OFFICER
QSPC	INTERNAL SPOOL USER PROFILE
QSRV	SERVICE USER PROFILE
QSYS	INTERNAL SYSTEM USER PROFILE
QSYSOPR	SYSTEM OPERATOR USER PROFILE
RMTUSER	REMOTE USER PROFILE
UNISAFE	INTERNAL SECURITY USER PROFILE
SFRPGM	SAFE/400 SECURITY OFFICER
UNISAFE400	ADMINISTRATOR USER PROFILE
ANTHONY	ANTHONY MASIELLO
BSAFEAUDIT	AUDITOR USER PROFILE
BSAFEADMIN	ADMIN USER PROFILE
LARRY	LARRY SCOTT

Additional configuration options on the right include 'Account Policy' (No account permissions defined), 'Idle Time (min)', 'Action', 'Send Message', 'Message Queue Library', and 'Message Queue'. Buttons for 'Apply', 'Undo', and 'Clear' are at the bottom.

Manejo de Sesiones Inactivas:

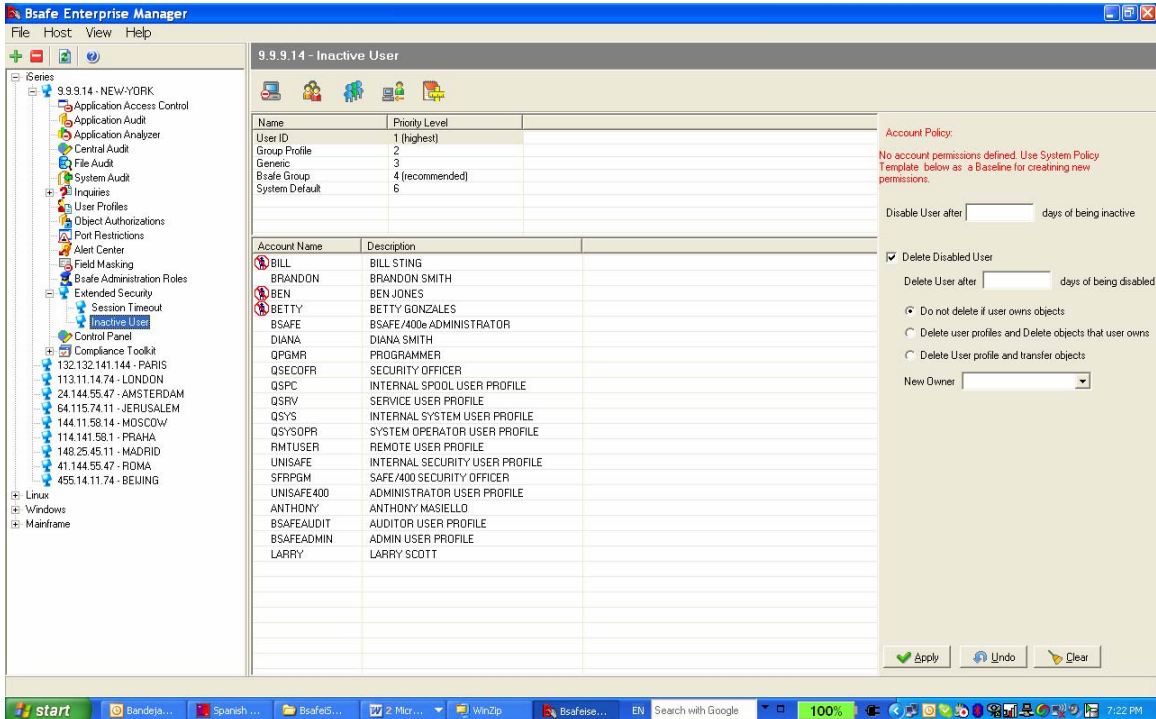
Bsafe/Enterprise Security ofrece una funcionalidad que permite el manejo de las sesiones de estaciones de trabajo inactivas, la cual se fundamenta en diferentes niveles de grupos de usuarios. Desde el nivel del sistema, luego a nivel de grupo de usuario, pasando luego al nivel de grupo de Bsafe hasta llegar al nivel de usuario individual.

Se puede especificar exactamente que acciones se van a tomar en caso de alcanzar el tiempo especificado, incluyendo envío de mensajes culminación del trabajo, desconexión del trabajo, o una combinación.

Utilizando los grupos de usuarios de Bsafe se puede crear un menor número de definiciones y aplicarlas de una manera más eficiente a un mayor número de usuarios para facilitar la implementación de esta funcionalidad.

Manejo de Usuarios Inactivos:

Bsafe/Enterprise Security permite monitorear los usuarios que están inactivos o que no hacen inicio de sesión durante un periodo de tiempo, y en paralelo se pueden ejecutar algunas acciones o tareas de acuerdo a las condiciones establecidas en la siguiente pantalla:



The screenshot shows the 'Bsafe Enterprise Manager' application window. The title bar reads '9.9.9.14 - Inactive User'. The interface is divided into several sections:

- Left Navigation Tree:** Shows a hierarchy of security features including Application Access Control, Application Audit, Application Analyzer, Central Audit, File Audit, System Audit, Inquiries, User Profiles, Object Authorizations, Port Restrictions, Alert Center, Field Masking, Bsafe Administration Roles, Extended Security, Session Timeout, Inactive User (selected), Control Panel, Compliance Toolkit, and various IP addresses for different locations (PARIS, LONDON, AMSTERDAM, JERUSALEM, MOSCOW, PRAHA, MADRID, ROMA, BEIJING).
- Top Section:** Contains a table for 'Priority Level' settings.

Name	Priority Level
User ID	1 (highest)
Group Profile	2
Generic	3
Bsafe Group	4 (recommended)
System Default	5
- Middle Section:** Contains a table for 'Account Name' and 'Description'.

Account Name	Description
BILL	BILL STING
BRANDON	BRANDON SMITH
BEN	BEN JONES
BETTY	BETTY GONZALES
BSAFE	BSAFE/400e ADMINISTRATOR
DIANA	DIANA SMITH
PGMGR	PROGRAMMER
QSECDFR	SECURITY OFFICER
QSPC	INTERNAL SPOOL USER PROFILE
QSRV	SERVICE USER PROFILE
QSYS	INTERNAL SYSTEM USER PROFILE
QSYSOPR	SYSTEM OPERATOR USER PROFILE
RMTUSER	REMOTE USER PROFILE
UNISAFE	INTERNAL SECURITY USER PROFILE
SFRPGM	SAFE/400 SECURITY OFFICER
UNISAFE400	ADMINISTRATOR USER PROFILE
ANTHONY	ANTHONY MASIELLO
BSAFEAUDIT	AUDITOR USER PROFILE
BSAFEADMIN	ADMIN USER PROFILE
LARRY	LARRY SCOTT
- Right Section:** Contains 'Account Policy' settings.

Account Policy:
No account permissions defined. Use System Policy Template below as a Baseline for creating new permissions.

Disable User after days of being inactive

Delete Disabled User

Delete User after days of being disabled

Do not delete if user owns objects

Delete user profiles and Delete objects that user owns

Delete User profile and transfer objects

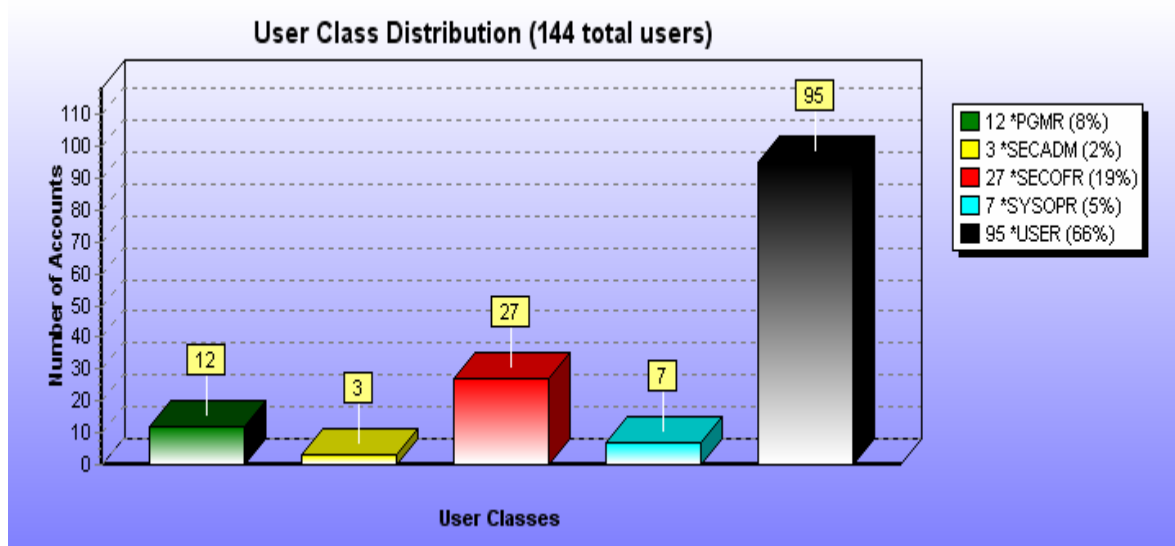
New Owner:
- Bottom:** Includes 'Apply', 'Undo', and 'Clear' buttons, and a Windows taskbar at the very bottom showing the Start button, taskbar, and system tray.

4.16. Análisis de Vulnerabilidad.

Bsafe/Enterprise Security permite generar un informe con todos los riesgos actuales, y algunas sugerencias para resolver los riesgos. A continuación se presentan algunos ejemplos:

Usuarios Poderosos por Clase de Usuarios

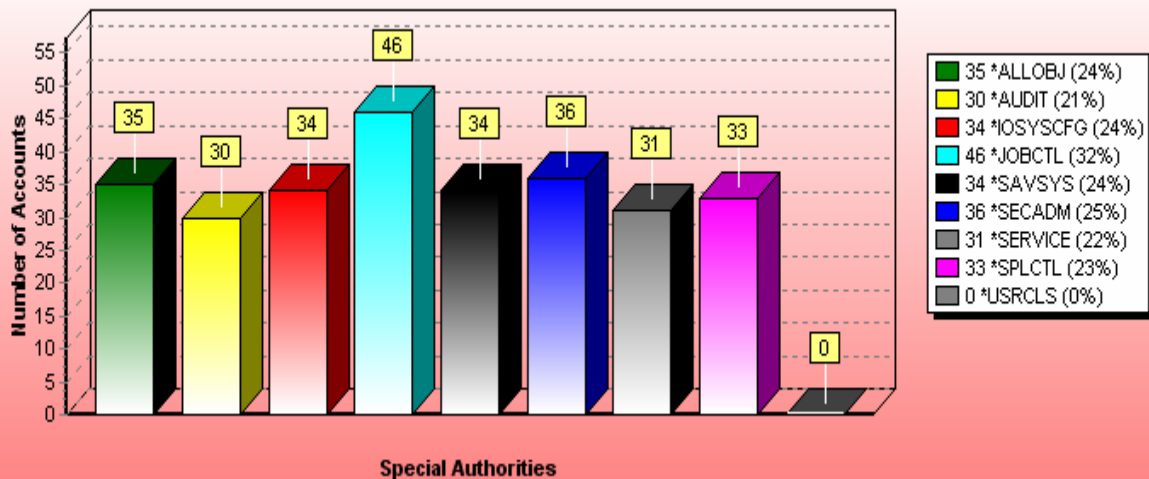
Clase de Usuarios	Descripción	Total	Porcentaje	Riesgo
✓ *PGMR	Programmer	12	8	
✓ *SECADM	Security Administrator	3	2	The number of users assigned as administrators is acceptable
⚠ *SECOFR	Security Officer	27	19	Too many users are assigned as security officers
⚠ *SYSOPR	System Operator	7	5	The number of users assigned as system operators is somewhat high
✓ *USER	User	95	66	
	All Users	144	100	









Usuarios Poderosos por Autorización Especial

Autorización	Descripción	Total	Porcentaje	Riesgo
⚠️ *ALLOBJ	All object authority	35	24	All objects authority granted to users not in class security Officer or Administrator
⚠️ *AUDIT	Audit authority	30	21	Auditing authority granted to users other than the system security officer
⚠️ *IOSYSCFG	Input/Output system configuration	34	24	I/O configurations authority given to users other than the system security officer
✅ *JOBCTL	Job control authority	46	32	No suggestions available
✅ *SAVSYS	Save system authority	34	24	No suggestions available
⚠️ *SECADM	Security administrator authority	36	25	Security administrator authority granted to users not in the same class
✅ *SERVICE	Service authority	31	22	No suggestions available
✅ *SPLCTL	Spool control authority	33	23	No suggestions available
✅ *USRCLS	Special authorities granted based on User Class	0	0	No suggestions available
	All Users	144	100	

Distribution of Special Authorities (144 total users)



Otros Usuarios con Riesgos de Clave (“Password”)

Descripción	Total	Porcentaje	Riesgo
 Powerful Users with default password	39	27	Default password are easy to guess
 Password same as Userprofile value	70	49	User & password are easy to guess
 IBM Pwd same as User Profile value	1	1	Change Default IBM supplied passwords
 Disabled Users	75	52	Disabled users require maintenance
 Previous SignOn	124	86	Previous users signon require maintenance
 SignOn Last Changed	136	94	Users needs to change passwords more often
All Users	144	100	

5. Beneficios para los Usuarios

- **Fácil de Utilizar.** **Bsafe/Enterprise Security** es el líder no nada más por sus múltiples funcionalidades, sino por la facilidad que ofrece su interfaz gráfica basada en Windows. Esta característica permite a los administradores experimentados y a los que no tienen conocimientos poder administrar la seguridad del sistema i de igual forma. Trabaja con el servidor HTTP incluyendo el último servidor i5 Apache.
- **En conformidad con** Sarbanes-Oxley, HIPAA, COBIT, Basle II, ISO 17799 y otros requerimientos de seguridad.
- **Máxima protección de los Sistemas i** a través del control flexible de los usuarios dentro y fuera de la organización incluyendo los usuarios no autorizados y usuarios poderosos.
- **Capacidades poderosas de auditoria** para identificar eventos y tendencias de acceso al sistema y a los datos.
- **Variedad de Reportes y Consultas** para cumplir con los requerimientos de auditoria.
- **Administración de las Políticas de Auditoria** se realizan de una manera sencilla a través de la interfaz intuitiva gráfica GUI.
- **Detección a tiempo** – a través del Sistema de Detección de Intrusos IDS el cual alertará los intentos de acceso no autorizados, los intentos de inicio de sesión y otras actividades en el momento en que ellas ocurran.
- **Una sola solución, integrada** – la cual abarca todas las funciones de seguridad: control de acceso de los puntos de salida, IDS, auditoria, definición de políticas y otras funciones principales de administración a través de una interfaz de PC gráfica intuitiva.
- **Reducción en la carga del servidor** después de eliminar todas las actividades que no están autorizadas.
- **El Retorno de la Inversión - ROI.** El costo de **Bsafe/Enterprise Security** es una fracción del costo que tiene la inversión en tiempo que toma un administrador para auditar, administrar investigar eventos sospechosos, detectar datos dañados, entre otros.